BAB I

PENDAHULUAN

1.1 Latar Belakang

Privasi adalah kebutuhan bagi setiap orang, dalam era teknologi seperti sekarang dimana smartphone atau handphone pintar mulai digunakan untuk kebutuhan sosial maupun bisnis, privasi seseorang sudah berkurang atau sulit untuk didapatkan. Para pemilik smartphone memasukkan berbagai jenis file kedalam HP (handphone) mereka, dan berpikir bahwa data yang ada dalam hp mereka aman dari orang lain, tentu saja hal itu benar selama tidak ada yang mencoba mencurinya, meminjamnya, atau "memata-matai". Pengguna smartphone yang menggunakan OS Android sekarang mencapai 68% dari total pengguna smartphone dunia dengan pesaingnya iOS apple sebesar 16.9% (IDC.com, 2012). Kelebihan perangkat Android dari para pesaingnya adalah banyaknya pembuat HP yang mengembangkan perangkat mereka dengan OS Android dan harga yang terjangkau oleh banyak pihak.

Keamanan data sangat penting terutama bagi pemakai yang menyimpan data pribadi mereka dalam perangkat mobile. Perangkat mobile seperti smartphone telah dilengkapi oleh *tools* atau kakas yang dapat membantu mengamankan perangkat pengguna, seperti PIN (personal id number) dan *pattern lock* (kunci pola) untuk mengunci HP atau membatasi akses. Namun hal tersebut hanya mengamankan perangkat HP tidak file yang ada pada kartu memory. File yang berada dalam memori tersebut dapat dengan mudah dibuka, dengan memindahkan kartu memory ke device lain. Pengamanan file dapat dilakukan dengan mengenkripsi file. Software enkripsi akan memproses file dan mengamankannya dengan kata kunci, namun kekurangan dari software terdapat pada penggunanya, dimana pengguna harus mengingat kata kunci tersebut. Apabila pengguna melupakan kata kunci, maka pengguna tidak dapat mengakses file yang telah terenkripsi.

Beberapa aplikasi tanpa berbayar yang telah dicoba oleh penulis yaitu Boxcryptor yang kelebihannya adalah dapat mengenkripsi dari berbagai sumber seperti dropbox, local storage, google drive dan cloud storage lainnya. Boxcryptor menggunakan password utama dalam mengenkripsi file dan pilihan untuk menggunakan PIN pada saat membuka aplikasi. Tidak adanya pengembalian password, ketika pengguna lupa maka password di reset. Ketika penulis menggunakan aplikasi ini, aplikasi ini tidak dapat mengenali tipe file png, bmp,

pdf dan doc/docx serta jpg dan jpeg padahal termasuk dalam file type yg didukung. Setelah itu Encdroid adalah aplikasi enkripsi file lain, Encdroid memiliki kelebihan yaitu dapat terkoneksi dengan cloud storage Dropbox. Encdroid mengkripsi "volume", seperti sebuah folder khusus untuk di enkripsi. Aplikasi ini tidak memiliki penanganan pengembalian password.

Penelitian tentang enkripsi file telah dilakukan dan dikembangkan oleh para peneliti dan developer dengan menggunakan beragam metode enkripsi. Metode yang digunakan beberapa tahun terakhir ini adalah enkripsi menggunakan metode AES. AES atau *Advance Encryption Standard* merupakan standar enkripsi lanjut yang digunakan oleh pemerintah untuk memproduksi standar enkripsi yang dapat digunakan para pengembang software dalam produksi produk mereka. AES terbaru diambil dari kontes yang diadakan NIST (National Institute of Standards and Technology), yang pemenang kontes tersebut adalah algoritma Rijndael (NIST 800-38A,2001). Aplikasi enkripsi yang berhubungan telah banyak menggunakan AES dalam penerapannya yaitu dengan AES-256. Beragam metode dan algoritma dalam persaingan AES telah diteliti dengan perbandingan performa pada berbagai prosesor, perbandingan antar metode AES 128, 192, dan 256. Kesimpulan dari penelitian adalah metode AES apabila semakin besar kunci yang diberikan maka semakin lama pemrosesannya, sehingga AES dengan kunci 128 merupakan yang tercepat (Scheier, Bruce – Whiting, Doug, 2000). Selain itu Team Twofish yang merupakan salah satu tim yang mengikuti kompetisi AES meneliti kembali kompetensi beragam metode yang ikut dalam kompetisi. Algoritma AES adalah standar kunci simetris yang diadopsi oleh pemerintah Amerika. AES yang disebut juga dengan Rijndael dikembangkan oleh Vincent Rijmen dan Joan Daemen dan dipublikasikan pada tahun 1998. Team Twofish meliti dalam faktor keamanan lima algoritma yang ditandingkan salah satunya AES, dalam performa hardware dan software AES memiliki kelebihan dan Serpent memiliki kelebihan dalam keamanan. (The Twofish Team Comments, 2000). Penelitian terbaru tentang AES adalah perbandingan antara DES, 3DES dan AES dari sembilan faktor yang diujikan dengan kesimpulan AES lebih baik dari dua algoritma lainnya. (Alanzi, Hamdan O., Zaidan B.B., 2010).

Dijelaskan diatas bahwa AES-128 bit memiliki keunggulan dalam hal kecepatan pemrosesan, tanpa harus mengurangi keamanan (Scheier, Bruce – Whiting, Doug, 2000). Sampai saat ini belum ada yang mampu menembus keamanan AES baik itu 128, 192 maupun 256. Untuk menembus keamanan AES 128 diperlukan waktu komputasi $2^{126.1}$ menggunakan serangan 7-round's. Sedangkan untuk AES 256 dibutuhkan waktu komputasi hampir dua kali lipat AES 128 dengan serangan 8-round's (Bogdanov,Andrey 2011). Untuk itu menurut penulis didukung dengan data yang telah disebutkan penggunaan AES

128 sudah memadai untuk tingkat personal, dimana data yang disimpan ada dalam perangkat dengan performa yang terbatas.

Dalam membuat software android yang berhubungan dengan pengolahan file dan pemberian password untuk proteksi, sering terjadi kesulitan untuk mengambil atau mendapatkan kembali file yang telah diproses, saat pengguna kesulitan dalam mengingat password yang diberikan kepada file. Solusi strategi yang saat ini digunakan adalah *sent to mail recovery*. Uraian dalam paragraf sebelumnya merupakan latar belakang penulis dalam proyek tugas akhir bidang kriptografi menggunakan AES-128 yang dianggap sebagai pemroses tercepat. Aplikasi ini diterapkan pada perangkat Android.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah maka dapat dibuat suatu rumusan masalah,

“Bagaimana cara melakukan pengamanan file menggunakan algoritma AES – 128 serta reset atau mengirimkan password kepada pengguna, pada saat pengguna tidak dapat mengingat password.”

1.3 Batasan Penelitian

1. Input berupa file teks, dan file gambar
2. Pengujian pada smartphone dengan OS Android 2.3.3 ke atas

1.4 Tujuan Penelitian

Tujuan dari penulisan ini adalah dihasilkan aplikasi yang dapat mengenkripsi dan mendekripsikan kembali file pada smartphone dengan OS Android dilengkapi dengan mekanisme pengembalian password yang relatif aman dan nyaman.

1.5 Sistematika Penulisan

BAB I Pendahuluan

Pada bab ini berisi penjelasan Latar Belakang, Rumusan Masalah, Batasan Penelitian, Tujuan Penelitian, dan Sistematika Penulisan.

BAB II Landasan Teori

Pada bab ini berisi penjelasan mengenai dasar teori teknologi yang digunakan dalam melaksanakan penelitian dalam tugas akhir ini.

BAB III Metodologi Penelitian

Bab ini membahas langkah-langkah yang dilaksanakan dalam proses penelitian dalam menyelesaikan kasus ini.

BAB IV Analisa dan Perancangan

Bab ini berisi pembahasan mengenai kebutuhan sistem, yang terdiri dari : *Flowchart system*, UML, *User interface*, perancangan menggunakan pendekatan berorientasi objek.

BAB Implementasi dan Pengujian

Bab ini menjelaskan mengenai implementasi penelitian dan eksperimen yang dilakukan dengan melakukan berbagai evaluasi dan perbaikan yang dirasa perlu berdasarkan hasil penelitian.

BAB VI Kesimpulan dan Saran

Bab ini membahas mengenai kesimpulan yang dihasilkan dari penelitian dan saran yang diperoleh untuk pengembangan lebih lanjut.